INCODING: Journal of Informatic and Computer Science Engineering
https://journal.mahesacenter.org/index.php/incoding/index || ISSN 2776-432X (online)
5 (1) 2025: 16-24
Genesis:
DOI: 10.34007/incoding.v5i1.775
Disubmit: 23 Januari 2025
Direview: 29 April 2025
Diterima: 30 April 2025

Data Security Application using Rivest Cipher 6 (RC 6) Algorithm

Robbi Rahim
Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia
*Coresponding Email: usurobbi85@zoho.com

Abstract

The prevention of misuse of data by other parties requires a good data security system. Cryptography is a means of securing data with a view to maintaining confidentiality of information contained in the data, so that information cannot be known to unauthorized parties. RC6 is a cryptographic block cipher algorithm that can be used to secure data or files from irresponsible parties. This study found that the data secured using the RC6 algorithm was quite good and required a long time for some parties to get the plain text.

Keywords: Security, Data Security, RC6, Algorithm

INTRODUCTION

Electronic communication such as SMS, e-mail, chat, web, e-banking and so on, has become a common way of communication today[1]. Data flows all the time through communication networks and some is very private data that should not be known by other parties. Meanwhile, data tapping on communication networks is a very possible thing to do[2], [3]. This will ultimately result in misuse of data by other parties who are not entitled.

A good data security system is needed to prevent misuse of data by other parties. Cryptography is a means of securing data with a view to maintaining confidentiality of information contained in the data, so that information can not be made known to unauthorized parties. In maintaining confidentiality of information, cryptography encodes plain text in an unrecognizable form of cipher text, and although other people will receive the data later, they can not understand its contents[4], [5].

The RC6 algorithm is a block cryptographic algorithm designed by Ronald L. Rivest, Matt J.B. Robshaw, Ray Sidney, and Yuqin Lisa Yin from RSA Laboratories. The algorithm is designed to be AES (Advance Encryption Standard). Although not chosen as AES, the RC6 algorithm is known for its simplicity and speed[6], [7].

RC6 algorithm in this study is used to secure data so that it is not easily known or read by irresponsible parties, but also made a prototype RC6 application that makes it easy to know how the security process using RC6 algorithm[8], [9].

RESEARCH METHOD

Cryptography

Cryptography is the method to encrypt messages / data / information by coding in order to make the message unreadable by person. Cryptography is intended to keep information contained in the data secret so that it is not exposed to unauthorized parties[10].

cryptography there are several terms that are often used, among others: plaintext, ciphertext, key, encryption and decryption. Plaintext is normal data / messages to be encoded. Ciphertext is data / encrypted message. Key is a series of characters that are confidential. Encryption is the process to encode a message or the transformation process from plaintext to ciphertext. In other words, encryption is the transformation of

data into a form that can hardly be read without sufficient and appropriate knowledge. The aim is to guarantee confidentiality by making the information hidden from anyone who is not the owner or who has no interest in the information, even for people who have access to encrypted data. Decryption is the process of returning encrypted messages to original messages or the process of transforming ciphertext back into plaintext. Or it can be interpreted that decryption is the opposite of encryption[11], [12].

In maintaining data confidentiality, cryptography transforms plaintext into an unrecognizable ciphertext. This ciphertext is then sent to the recipient. After reaching the recipient, the ciphertext is transformed back into its original plaintext form so that it can be understood.

Symmetric Algorithm

Symmetric encryption algorithms are algorithms that use the same key for encryption and decryption[13].

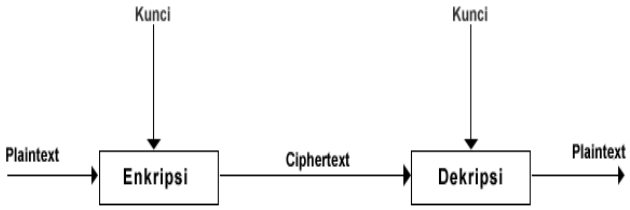

Fig 1. Symmetric Process

The symmetric algorithm can be divided into 2 categories namely Block Ciphers and Stream Ciphers. Block ciphers are encryption schemes that break plaintext into blocks of a certain length which are then encrypted. In block ciphers, the coding process is oriented to a set of bits or bytes of data (per block). Collection of these bits is called a block. While on stream ciphers, the encoding process is done bit by bit. Block ciphers are generally used for large data sizes while stream ciphers are used for smaller data sizes.

Asymmetric Algorithm

Asymmetric encryption algorithms are algorithms that use a number of keys to encrypt and decrypt[14]. This algorithm is often known as a public key algorithm since the encryption key is freely accessible or known to everyone, but only those who are allowed to know or also call a private key are aware of the key to decryption. Figure 2 demonstrates the asymmetrical encryption-decryption algorithm.

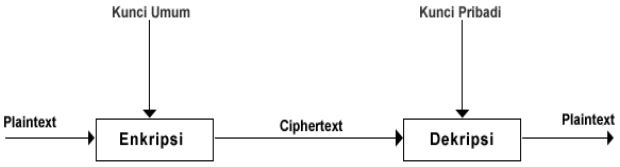

Fig 2. Asymmetric Process

In this public key algorithm, anyone can encrypt data using public keys that are generally known. However, the encrypted data can only be decrypted using a private key that is only known by the recipient.

RC6 Algorithm

The RC6 algorithm is a block cipher cryptographic algorithm designed by Ronald L. Rivest, Matt J.B. Robshaw, Ray Sidney, and Yuqin Lisa Yin from RSA Laboratories. This algorithm is designed to be AES (Advance Encryption Standard)[9].

The RC6 algorithm is an algorithm with full parameters and is specified with the RC6-w / r / b notation. Where w is the size of the word in bits. The parameter r indicates the number of iterations during the encryption process, where r cannot be negative and b is the key length in bytes. After this algorithm is included in the AES candidate, it is determined that the values of w = 32, r = 20 and b vary between 16, 24 and 32 bytes. This algorithm works with four w-bit registers. In accordance with the AES 128-bit block size, the w value is 32 bits.

The RC6 algorithm divides the plaintext of 128-bit blocks and then splits each 128-bit block into four registers A, B, C, D, each of which is 32 bits in size, so that the 4 registers will be filled by plaintext which will then be used during the process encryption

and after the encryption process ends the contents of the registers are ciphertext. In RC6 there is no Feistel Network found in DES, but the function f (x) = x (2x + 1) and shifting 5 bits to the left is applied.

The RC6 algorithm's encryption and decryption process uses six basic operations:

a + b = addition of integer modulus 232

a - b = reduction of integer modulus 232

a b = exclusive-or bitwise operation

a * b = integer modulus multiplication operation 232

a <<< b = right-hand rotation of the word w-bit a least significant number of lg w bits of b

a >>> b = right-word rotation w-bit a least significant number of lg w bits from b

Where lg w is the base two logarithm of w.

In the process of encryption and decryption of the RC6 algorithm internal subkeys (S arrays) are derived from the user key (K) by using the RC6 algorithm's internal subkey formation process.

RC6 Encryption

The encryption process with the RC6 algorithm starts with breaking 128-bit blocks into 4 32-bit blocks, each in registers A, B, C and D. The encryption process that occurs in the RC6 algorithm is shown in Figure 3.

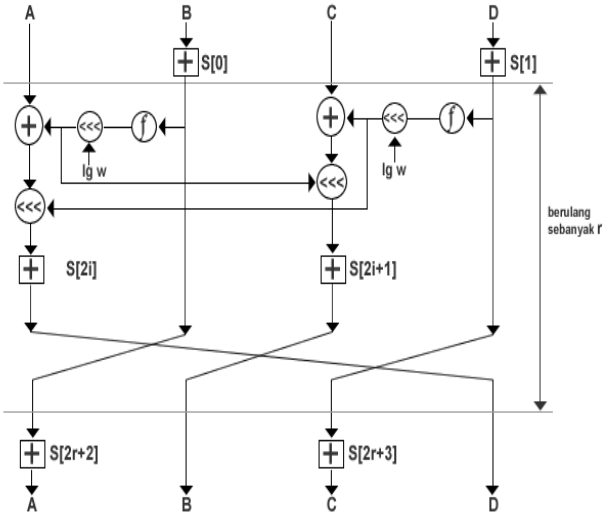

Fig 3. RC6 Encryption

The RC6 algorithm uses 44 subkeys (with r=20) generated from the key, named S[0] to S[43]. Each subkey has a length of 32 bits.

After the 128-bit block is divided into four 32-bit registers A, B , C and D, the encryption process begins and ends with a whitening process aimed at concealing the first and last iteration of the encryption process.

In the initial whitening process, the value of B is added to S[0] and the value of D is added to S[i]. 2 subkeys are used in each iteration on RC6. The subkeys used in the first iteration are S[2] and S[3], while the following iterations are followed by the subkey. After completion of the 20th iteration, the final whitening process is carried out where the value of A is added to S[42] and the value of C is added to S[43].

Each iteration of the RC6 algorithm follows the following rules, the value of B is entered into the function f, which is defined as f(x) = x (2x + 1), and then rotates to the left as far as lg w or 5 bits. The results obtained in this process are expected to be u. The value of u is then XORed with C and the result is the value of C. The value of t is also used to rotate the value to the left as a reference for C. The same applies to the value of u, also used as a reference for the value of A to the left spinning process.

RC6 Decryption

The RC6 algorithm's cipher-text decryption process is a reversal of encryption process. If the encryption process uses additional operations, the decryption process uses a subtraction operation. Subkeys used in the whitening process after the last iteration are used before the first iteration, and vice versa, used in the whitening process before the first iteration after the last iteration. Consequently, to do the decryption, all you have to do is apply the same encryption algorithm, with each iteration using the same subkey used during the encryption, only the order of the subkeys used is reversed. Figure 4 demonstrates the RC6 algorithm decryption method.

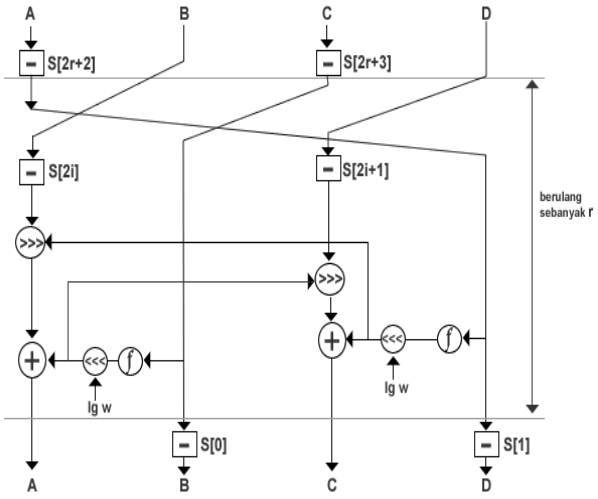

Fig 4. RC6 Decryption

RESULT & DISCUSSION

The following is an RC6 key expansion algorithm to generate subkeys that will be used for the encryption and decryption process. The following is an algorithm to encrypt according to the RC6 algorithm with the input of four 32-bit plaintext blocks (BlokP1, BlokP2, BlokP3, BlokP4)

Begin

BlokP2 = BlokP2 + S[0]

BlokP4 = BlokP4 + S[1]

for i = 1 to r do

t = (BlokP2 * (2 * BlokP2 + 1))<<< lg w

u = (BlokP4 * (2 * BlokP4 + 1))<<< lg w

BlokP1 = ((BlokP1 $\oplus$ t)<<< u) + S[2i]

BlokP3 = ((BlokP3 $\oplus$ u)<<< t) + S[2i+ 1]

(BlokP1, BlokP2, BlokP3, BlokP4) = (BlokP2, BlokP3, BlokP4, BlokP1)

endfor

BlokP1 = BlokP1 + S[2r + 2]

BlokP3 = BlokP3 + S[2r + 3]

End

The following algorithm performs the reading process of ciphertext files up to 128 bits (16 bytes), then invokes the decryption of the RC6 algorithm.

Begin

BlokC3 = BlokC3 - S[2r + 3]

BlokC1 = BlokC1 - S[2r + 2]

for *i = r* ***downto*** *1* ***do***

(BlokC1, BlokC2, BlokC3, BlokC4) = (BlokC4, BlokC1, BlokC2, BlokC3)

*u = (BlokC4 * (2* BlokC4 + 1))<<< lg w*

*t = (BlokC2 * (2 *BlokC2 + 1))<<< lg w*

BlokC3 = ((BlokC3 - S[2i + 1])>>>t) $\oplus$ *u*

BlokC1 = ((BlokC1 - S[2i])>>>u) $\oplus$ *t*

endfor

BlokC4 = BlokC4 - S[1]

BlokC2 = BlokC2 - S[0]

End

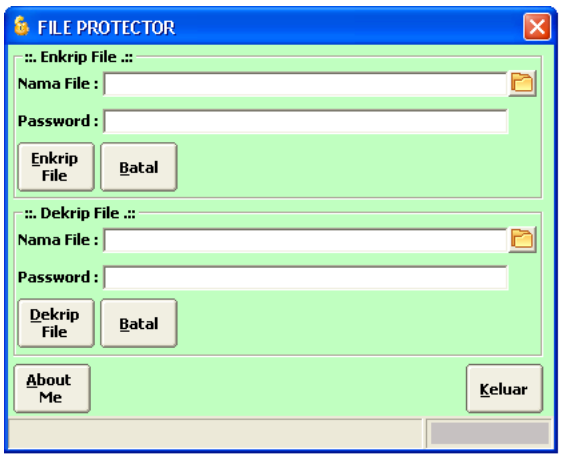

Fig 5. RC6 Application

CONCLUSION

After doing the design and implementation, the authors can provide some conclusions as follows:

a.This application is useful for securing data files with encryption techniques, so that the data files are scrambled after the encryption process and then the data is stored or sent through network media.

b. Data files that have been encrypted or encrypted can be changed again to their original form or (decryption) that is easily understood

c. File size after encryption is affected by adding blank characters.

d. The use of different keys to encrypt the same file, will produce a different ciphertext.

e.The size of the key does not affect the file size after the encryption and decryption process.

REFERENCE

[1] S. D. Shyamlee and M. Phil, ""Use of Technology in English Language Teaching and Learning": An Analysis."

[2] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: The internet of things architecture, possible applications and key challenges," in *Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012*, 2012, pp. 257–260.

[3] D. Asteria, E. Suyanti, D. Utari, and D. Wisnu, "Model of Environmental Communication with Gender Perspective in Resolving Environmental Conflict in Urban Area (Study on the Role of Women's Activist in Sustainable Environmental Conflict Management)," *Procedia Environ. Sci.*, vol. 20, pp. 553–562, 2014.

[4] J. A. Alzubi *et al.*, "Hashed Needham Schroeder Industrial IoT based Cost Optimized Deep Secured data transmission in cloud," *Measurement*, vol. 150, p. 107077, Jan. 2020.

[5] R. Rahim, E. F. Armay, D. Susilo, R. F. Marta, and A. Alanda, "Cloud computing security issues and possibilities," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 6 Special Issue, pp. 927–931, Aug. 2019.

[6] A. L. Biel, "How brand image drives brand equity," *J. Advert. Res.*, vol. 32, pp. RC6–RC12, 1992.

[7] I. Halik and Y. Prayudi, "Studi dan Analisis Algoritma Rivest Code 6 (RC6) dalam Enkripsi/Dekripsi Data," *Stud. Dan Anal. Algoritm. Rivest Code 6 Dalam Enkripsi/Dekripsi Data*, vol. 6, no. D, pp. 149–158, 2005.

[8] T. Iwata and K. Kurosawa, "On the pseudorandomness of the AES Finalists - RC6 and serpent," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2001.

[9] H. E. H. Ahmed, H. M. Kalash, and O. S. Farag Allah, "Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images," in *2007 International Conference on Electrical Engineering, ICEE*, 2007.

[10] E. Bertino and E. Ferrari, "Information security," in *The Practical Handbook of Internet Computing*, 2004.

[11] W. Stallings, *Network security essentials : applications and standards*. 2011.

[12] W. Stallings, "Cryptography and Network Security Principles and Practices," 4th Editio., .

[13] J. Hoffstein, J. C. Pipher, and J. H. Silverman, *An Introduction to Mathematical Cryptography*. Springer, 2008.

[14] M. Ebrahim, S. Khan, and U. Bin Khalid, "Symmetric Algorithm Survey: A Comparative Analysis," vol. 61, no. 20, pp. 12–19, 2014.